Euclidean domains and UFDs

In this lecture we take a closer look at the Gaussian integers

$$\mathbb{Z}[i] = \{a + b\sqrt{-1} : \ a, b \in \mathbb{Z}\}$$

This ring appears to be closely related to the integers $\mathbb{Z}$; after all, we have only thrown in the element $i = \sqrt{-1}$. So how much of what is true for the ring of integers is true for the Gaussian integers? One of the most important properties of $\mathbb{Z}$ is the following:

▸ **Fundamental Theorem of Arithmetic (FTA): Let n be a positive integer. Then there are (not necessarily distinct) prime numbers $p_1, \ldots, p_m$ such that**

$$n = p_1 p_2 \cdots p_m$$

If $n = q_1 \cdots q_l$ for other primes q_i then $l = m$ and $q_i = p_i$ after re-labelling.

Can we obtain a similar statement for $\mathbb{Z}[i]$? One thing to note is the equation

$$(1 + i)(1 - i) = 1^2 - i^2 = 2$$

and $1 \pm i$ are not units in $\mathbb{Z}[i]$. In other words, "2" is not "prime" in this ring. Thus even if we do have some kind of FTA for $\mathbb{Z}[i]$, the factorizations will be different than those of $\mathbb{Z}$.

First we will formalize the kind of structure we are after. An *irreducible* element $a \in R$ in an integral domain R is an element that is non-zero and not a unit, and such that if $a = bc$, then one of b or c is a unit. Heuristically, a cannot be "decomposed" into smaller pieces. The irreducible elements of $\mathbb{Z}$ are exactly the prime numbers and their negatives.

▸ **An integral domain R is a *Unique Factorization Domain* (UFD) if every non-zero $a \in R$ is the product of (not necessarily distinct) irreducible elements $p_i \in R$:**

$$a = p_1 p_2 \cdots p_m$$

This representation of a is unique in the sense that if $a = q_1 \cdots q_n$ for irreducibles q_i, then after re-ordering the q_i's we have $m = n$ and $q_i = u_i p_i$ for some units u_i.

Thus a UFD is a ring in which we have a generalized version of the FTA.

Now we can rephrase our above question: is the ring $\mathbb{Z}[i]$ a UFD? This question is closely related to PID's because of the following.

▸ **If R is a PID then it is a UFD.**

For the sake of time we will omit the proof, although it is not beyond the scope of the course.

To get "unique factorization" for Gaussian integers, we may hope to show $\mathbb{Z}[i]$ is a PID.

In search of some inspiration, we return to our proof that for R a field, $R[x]$ is a PID. How did we accomplish this? The key to the proof was the division algorithm: for any $f(x), g(x) \in R[x]$ with $g(x)$ non-zero, there are $q(x), r(x) \in R[x]$ such that

$$f(x) = g(x)q(x) + r(x)$$

and such that either $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$. With this, given any non-zero ideal $I \subset R[x]$ we saw that for any polynomial $f(x) \in I$ that was of minimal degree among all non-zero elements in I, we have $I = (f(x))$, and thus I is principal.

The general structure of this proof can be abstracted. For a general integral domain R, what we need in order to abstract this proof is an analogue of the "degree" of elements.

▸ **An integral domain R is a *Euclidean Domain* if there is a function $N : R\backslash\{0\} \to \mathbb{Z}_{\geqslant 0}$ such that for all $a, b \in R$ with $b \neq 0$ there are $q, r \in R$ such that**

$$a = bq + r$$

where either $r = 0$ or $N(r) < N(b)$.

In other words, a Euclidean domain is an integral domain where we have an abstracted version of the division algorithm. The function N replaces "deg" in our example above.

▸ **If R is a Euclidean domain then R is a PID.**

Proof. As remarked above, the proof is the same as showing that the ring of polynomials over a field is a PID. First, we take a non-zero ideal $I \subset R$ in our Euclidean domain R. Then let $a \in I$ be such that $N(a)$ is minimal among all non-zero elements in I. Finally, you can show that $I = (a)$ just as in the polynomial case, replacing "deg" by "N" throughout. □

▸ **The ring of Gaussian integers $\mathbb{Z}[i]$ is a Euclidean domain.**

Proof. We must find a suitable function N from non-zero elements of $\mathbb{Z}[i]$ to the non-negative integers. For this function we take the complex norm squared:

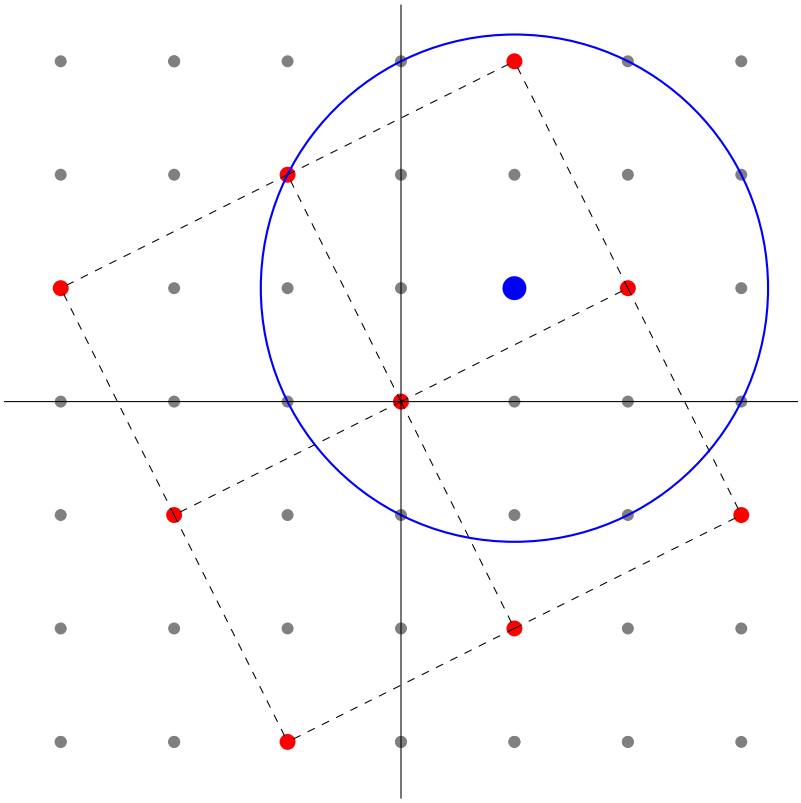
$$N(a + bi) = |a + bi|^2 = a^2 + b^2$$

Now we must show that given $x = a + bi$ and $y = c + di$ in $\mathbb{Z}[i]$ with $y \neq 0$ we can find $q, r \in \mathbb{Z}[i]$ such that $x = yq + r$ and either $r = 0$ or $N(r) < N(y)$. This last condition is equivalent to the condition $|r| < |y|$.

Thus what we are after is: given $x, y \in \mathbb{Z}[i]$, find some $q \in \mathbb{Z}[i]$ such that $|yq - x| < |y|$. For then we can take $r = yq - x$ and we are done.

Let us consider the principal ideal $I = (y) = \{yz : z \in \mathbb{Z}[i]\}$. Note $yi = (c + di)i = ci - d$ is the point in the complex plane which is y rotated by 90° counter-clockwise. Furthermore, any other element in I is of the form $my + nyi$ where $n, m \in \mathbb{Z}$. Thus the elements of I form a square "lattice" in the complex plane.

Now x is inside one of the squares in this lattice. Note that there is a corner of the square whose distance from x is at most $|y|\sqrt{2}/2 < |y|$. (Here we use that a square of side lengths R has diagonal of length $\sqrt{2}R$.) In particular, the disk of radius $|y|$ centered at x contains one of the corners of the square. Therefore there is some point qy in I that lies in this disk around x. Since it is in this disk it satisfies $|qy - x| < |y|$, which is what we wanted.



The argument is illustrated in the figure above for a specific case, in which $y = 2 + i$ and $x = 1 + i$. The red dots are the ideal I, and the blue dot is x. In fact in this case you can see that the origin is in the disk around x, and we can take $q = 0$. □

We have now achieved our original goal, of showing that $\mathbb{Z}[i]$ has "unique factorization":

▶ **The ring of Gaussian integers $\mathbb{Z}[i]$ is a UFD.**

This follows from our result that a Euclidean domain is a UFD.

For example, a factorization of $5 \in \mathbb{Z}[i]$ is given as follows:

$$5 = (2 + i)(2 - i)$$

Furthermore, $(2+i)$ and $(2-i)$ are irreducibles, so this is the "unique factorization" of 5 in this ring. We also have the factorization

$$5 = (1-2i)(1+2i)$$

However the factors are related by units: $(2+i) = i(1-2i)$ and $(2-i) = -i(1+2i)$.

On the other hand, 3 remains "prime" in this ring, and does not factor into smaller irreducible parts. It can be shown that the only prime numbers $p \in \mathbb{Z}$ which are still "prime" (i.e. irreducible) in the ring $\mathbb{Z}[i]$ are the primes p such that $p \equiv 3 \pmod 4$.

Example: Consider the ring $\mathbb{Z}[\sqrt{-5}]$. This is *not* a UFD! In fact we have

$$6 = (2)(3) = (1+\sqrt{-5})(1-\sqrt{-5})$$

These are two different factorizations of 6 in this ring. Note that the units of this ring are $\{1, -1\}$, so these factorizations are truly distinct. The failure of $\mathbb{Z}[\sqrt{-5}]$ to be a UFD is related to (but not implied by) the fact that it is not a PID.